

WHAT IS CLAIMED IS:

1. A system for providing biometric authentication, the system using a Web cloud as a communication medium, the system comprising:
- at least one Web client station linked to the Web cloud, the Web client station providing selected live data respecting biometric characteristics of an individual who is using the Web client station;
- at least one Web server station linked to the Web cloud, access of the Web server station via the Web cloud being sought by the individual using the Web client station and being dependent on authentication of the individual; and
- an authentication center linked to at least one of the Web client and Web server stations so as to receive the live data, the authentication center having records of biometric data of one or more enrolled individuals, the authentication center providing for comparison of the live data with selected records, the comparison being to determine whether the live data sufficiently matches the selected records as to authenticate the individual seeking access.
2. A system as claimed in Claim 1, wherein the Web client stations and the Web server stations are linked to the Web cloud via Web connections, the Web connections supporting a secure transport protocol.
3. A system as claimed in Claim 2, wherein the authentication center is linked to at least one of the Web client stations and Web server stations via authentication center connections, the authentication center connections supporting a secure transport protocol.
4. A system as claimed in Claim 3, wherein at least one of the Web connections and the authentication center connections support HTTP.

BEST AVAILABLE COPY

5. A system as claimed in Claim 3, wherein the authentication center connections are not via the Web cloud.
- 5 6. A system as claimed in Claim 1, wherein one or more of the Web client stations comprise a Web client and a biometric I/O device, the biometric I/O device acquiring data respecting biometric characteristics of the individual and the Web, and the Web client being linked to the biometric I/O device for receiving the acquired data or data representative thereof.
- 10 7. A system as claimed in claim 6, wherein the Web client comprises an interface mechanism, the interface mechanism being associated with one or more biometric characteristics, and controlling the biometric I/O device based on one or more parameters associated with biometric authentication, the parameters being provided from at least one of the Web server station, the authentication center and the Web client station.
- 15 8. A system as claimed in claim 7, wherein either or both of the Web client and the interface mechanism comprise, respectively, software programs, the software programs being any combination of destructive or non-destructive.
- 20 9. A system as claimed in claim 7, wherein the Web server station comprises a Web server, the Web server providing some or all of the parameters associated with biometric authentication.
10. A system as claimed in claim 9, wherein the authentication center comprises an authorization server linked to one or more biometric servers, each of the biometric servers being linked, respectively, to one or more biometric databases, the biometric databases being captive.
- 25 11. A system as claimed in claim 9, wherein the authentication center comprises an authorization

server linked to one or more biometric servers, each of the biometric servers being linked, respectively, to one or more biometric databases, at least one of the biometric databases being independent.

12. A system as claimed in claim 1, wherein the Web server station comprises a Web server, the Web server providing to the Web client station parameters associated with biometric authentication.

13. A system as claimed in claim 1, wherein the authentication center comprises an authorization server linked to one or more biometric servers, each of the biometric servers being linked, respectively, to one or more biometric databases.

14. A system as claimed in claim 13, wherein at least one of the biometric servers is independent.

15. A system as claimed in claim 1, wherein the Web client station provides for the individual to have a claimed identity, and the authentication center supports (i) receiving said claimed identity, (ii) providing the selected records based on said claimed identity and (iii) comparing the live data with the so-provided, selected records.

16. A method for Web-based, biometric authentication of individuals who are using a Web client station, the individuals seeking access of a Web server station, the method comprising the steps of:

establishing parameters associated with selected biometric characteristics to be used in authentication;

acquiring, at the Web client station, biometric data in accordance with the parameters;

receiving, at an authentication center, a message that includes live data;

selecting, at the authentication center, one or more records from among records

associated with one or more enrolled individuals; and

comparing live data with selected records, the comparison determining whether the so-compared live data sufficiently matches the selected records as to authenticate the individual seeking access.

5 17. A method as claimed in claim 16, further comprising the steps of:

providing, at the Web client station, a claimed identity associated with the individual;

receiving, at the authentication center, a message that includes the claimed identity;

determining the acceptability of the message based on the claimed identity;

10 if the message is acceptable, providing, at the authentication center, selected records that agree with the claimed identity; and

comparing the received data with the so-provided, selected records.

15 18. A method as claimed in claim 16, further comprising the step of providing, from the authentication center, a response respecting the result of the comparing step, this providing step comprising the steps of:

(A) preparing the response, which step includes one or more of the following steps:

(i) preparing a digital certificate;

20 (ii) preparing a page having electronic links to accessible pages associated with one or more application servers;

(iii) preparing an appropriate entry in a biometric database; and

(iv) preparing a secure protocol message; and

(B) effecting the response, which step includes one or more of the following steps:

(i) downloading the response to the Web server station;

25 (ii) routing the response to the Web server station via the Web client station;

(iii) making an appropriate entry in a selected biometric;

(iv) downloading the response to the Web client station; and

BEST AVAILABLE COPY

(v) routing the response to the Web client station via the Web server station.

19. A method as claimed in claim 18, wherein the step of preparing a page having electronic links comprises including or activating only those electronic links that are appropriate to the confidence level attained in the comparing step.

20. A method as claimed in claim 16, further comprising the step of establishing secure communication channels in and among the Web client station, the Web server station and the authentication station.

21. A method as claimed in claim 20, wherein the step of establishing secure communication channels comprises:

(A) employing a Web client at the Web client station and a Web server at the Web server station, the Web client and the Web server providing for establishing a secure communication channel between the Web client station and the Web server station; and

(B) employing an interface mechanism at the Web client station and an authorization server at the authentication center, the interface mechanism and the authorization server providing for establishing a secure communication channel between the Web client station and the authentication center.

22. A method as claimed in claim 16, further comprising the step of recording selected details of the received message and the results of the comparing step so as to create a biometric audit trail.

23. A method as claimed in claim 22, further comprising the steps of using selected details of the received message, and comparing said selected details with a plurality of records, the

comparison determining whether the so-compared selected details sufficiently match any one or more of the so-compared records, so as to identify the individual seeking access of the Web server station.

24. A method as claimed in claim 16, wherein:

the acquiring step comprises plural acquisitions, said plural acquisitions relating to one or more biometric characteristics; and

the establishing parameters step further comprises at least one of the following steps:

(i) selecting a confidence level from among supported confidence levels, said supported confidence levels being categorized in relation to authentication based on using biometric data associated with single biometric characteristics and with combinations of biometric characteristics; and

(ii) selecting a trigger event, said trigger event causing the acquisition of biometric data.

25. A method as claimed in claim 24, wherein the step of selecting a trigger event comprises selected a time interval for repeating the authentication steps.

26. A method as claimed in claim 16, wherein the step of establishing parameters comprises one or more communications by and among the Web server station, the Web client station and the authentication center.

27. A method as claimed in claim 26, wherein the step of establishing parameters further comprises the step of choosing among negotiable parameters by using predetermined arbitration algorithms.

28. A method as claimed in claim 26, wherein the step of establishing parameters further

comprises downloading a page from the Web server station to the Web client station responsive to the Web client station requesting access of the Web server station, the page including parameters.

- 5      29. A method as claimed in claim 28, wherein the step of downloading a page from the Web server station comprises the step of including parameters that offer alternatives, the alternatives being selectable
30. A method as claimed in claim 16, further comprising the step of determining an authentication center from among plural authentication centers.

10

add  
D/C

BEST AVAILABLE COPY